April 26, 2023

by Verilog Solutions

TLDR

This research is aiming to be an easy-to-understand guide for everyday on-chain users on:

what is MEV

the lifecycle of a block-building process

the status quo of the MEV economics

some interesting ideas and discussions about the MEV

how to reduce your MEV exposure

MEV supply chain

MEV supply chain can be broken down into multiple segments, including wallet, RPC provider, searcher, builder, relay, and validators

Players in each segment compete both horizontally (against other players in the same segment) and vertically (against players in the upstream and downstream)

Each segment has its own unique ways of developing moat and varying degrees of the barrier of entry

There are also possibilities for horizontal and vertical integration within and across different segments

Not all MEVs are bad and malicious

Good side: Several DeFi projects depend on economically rational participants to maintain the effectiveness and stability of their protocols. One example is that decentralized exchange arbitrage, as a form of MEV opportunity, makes the market efficient by removing price discrepancies across different DEXes. In addition, back-running Oracle updates to quickly liquidate at-risk lending positions is a form of MEV opportunity that makes lending protocols economically solvent

Bad side: Some MEV opportunities such as sandwiching are malicious and harms the user’s economic benefits. Sandwiching victims often encounter greater slippage and poorer trade execution.

1. Introduction

Maximal Extractable Value (MEV) refers to the maximum value a blockchain miner or validator can make by including, excluding, or changing the order of transactions during the block production process.

The term MEV, originated during the Proof-of-Work era of Ethereum when miners controlled which blocks and transactions were inserted into the blockchain. Ethereum’s move to Proof-of-Stake (PoS) saw power over block proposal transition from miners to validators, but the pursuit of profit through manipulating transactions remained, so now the term “Maximal Extractable Value” is used.

MEV and transaction reordering are not just explained as a theoretical concept, but as a dynamic that is already occurring at scale in the form of transaction frontrunning on decentralized exchanges and which can have a significant impact on the user experience. From what has been able to be uncovered, over $908.3 million worth of MEV has been extracted since 2020. Quantifying the exact amount of MEV is challenging, given that many extraction techniques are designed to be concealed to maintain a competitive advantage.

MEV occurs when block producers in a blockchain (e.g. miners, validators) are able to extract value by arbitrarily reordering, including, or excluding transactions within a block, often to the detriment of users. Simply put, block producers can determine the order in which transactions are processed on the blockchain and exploit that power to their advantage.

The key players involved in MEV are wallets, searchers, validators, mempools, and relays .

View original

Credit: The MEV Supply Chain: a peek into the Future of this Industry by Thegostep and Flashbots

Wallet

A wallet is a digital or physical device that stores your private keys, which are used to access and manage cryptocurrency and blockchain-based assets, like NFTs. Most of the on-chain interactions for regular users are achieved through wallets.

Searchers

Searchers are individuals who interact with the mempool to monitor unconfirmed transactions and gain insight into imminent transactions before they are permanently recorded on the blockchain. Searchers implement algorithms that identify MEV opportunities from the pending transactions and generate transactions that extract value from found opportunities, such as front-running.

Validators

Validators are digital entities that are responsible for storing data, processing transactions, and proposing blocks to the blockchain. They are essential for ensuring the network's security and stability and are incentivized by staking typically 32 ETH.

Mempools

Mempools reside within nodes, acting as a holding memory pool of pending transactions waiting to be added to the blockchain. Note that there are public mempools exposed to everyone and private mempools exposed only to permitted entities. Transactions in a mempool are prioritized by fee, where a higher transaction fee increases the likelihood of a quicker inclusion into the blockchain, however, it is ultimately up to the block builder to determine the order of transactions being included in the next block.

Relays

A relay is a third-party intermediary between validators and block builders, relays provide block escrow service, which prevents validators from stealing MEV opportunities. It should be noted that relays are centralized at the current moment, and relays hold the power to censor transactions.

1. Different Types of MEV

2.1 Frontrunning

Front-running is the process by which an adversary observes transactions on the network layer and then acts upon this information by, for instance, issuing a competing transaction, with the hope that this transaction is mined before a victim transaction. It’s called front-running because the MEV searcher is trying to execute its own transaction before the victim transaction. An interesting note is that front-running is illegal in traditional finance as it breaks the fairness of the market.

2.2 Backrunning

Back-running occurs when a transaction sender wishes to have their transaction ordered immediately after some unconfirmed "target transaction". MEV searcher can finely control the order of transactions and ensure that its own transaction is ordered after the target transaction by submitting a transaction bundle. Some examples are:

The second transaction of a sandwich attack

Cross-DEX arbitrage

Liquidation after a price Oracle update

View original

Credit to: Demystify the dark forest on Ethereum — Sandwich Attacks by Liyi Zhou

As can be seen in the above picture, Tv is the target transaction intended to trade X for Y. Both TA1 and TA2 are transactions that are executed by the attacker. In this case, TA1 is performed in a front-running fashion trading X for Y to increase the price of asset Y. On the other hand, TA2 is executed after Tv (the target transaction). This transaction trades Y for X to recover the initial position after making a profit.

2.3 Just-in-Time Liquidity (JIT)

JIT is a type of on-chain liquidity provision behavior where an LP mints and burns a concentrated position immediately before and after a trade has been swapped. It has also been considered a type of sandwich attack that usually happens on Uniswap V3, below is an example:

Alice wants to swap 1000 ETH → 2.2 million USDC, the transaction has been sent to the public mempool.

Searchers found the pending tx, and this searcher is looking for opportunities to buy ETH for a lower price to perform more arbitrage. Thus, he sends:

1st transaction quickly flashloan huge amount of ETH and USDC & provided concentrated liquidity on Uni V3

2nd transaction after Alice executes the transaction of sell to withdraw liquidity and return all the fund

In this scenario:

Searcher found the opportunities to get ETH at a low cost

Searchers also enjoyed high trading fees paid by Alice

Alice enjoyed low slippage

Overall, JIT is neutral, the dark side lies in taking away the huge portion of fees that LP, who have been providing liquidity consistently, should earn, while the bright side is this behavior benefits the trader to have lower slippage.

2.4 Time-Bandit Attack

View original

Credit: What is MEV? A Simple Guide by RILEY

Time-Bandit Attack is a theoretical attack model. We illustrate a scenario with the above diagram. Let's assume Jane and George are two large miners in the market, and they are both mining the next three blocks of ETH.

The block reward for each block is roughly around $100.

When mining the first block, George suddenly discovers a $1000 arbitrage and MEV opportunity.

Rationally, George will choose to rework Block 4 and 5 that Jane has already mined, including his own arbitrage space, and mine the next block in advance. Therefore, George decides to rework Block 4.

After the reorganization, George now has the longest chain and can directly obtain the block reward for Block 6.

However, in this event, George may need to borrow some computing power from other platforms and miners in the short term. Such an MEV attack scheme is more applicable in a POW environment. In Ethereum with Tendermint or POS, this type of MEV will be greatly reduced.

1. Wallet/Builder/Proposer/Searcher Economic s

3.1 Different players in the MEV supply chain

View original

Credit: The MEV Supply Chain: a peek into the Future of this Industry by Thegostep and Flashbots

When a transaction is sent by a user, the transaction might go through a journey and be passed around to different players depicted above.

For example, when a user wishes to swap 10 ETH for USDC on Uniswap, the transaction is first composed by the wallet and signed by the user.

The signed transaction is then sent to the mempool of the RPC that the wallet is connected.

” Flashbots Protect ” in the above picture is an RPC provider, and it provides private mempool access to the trusted searcher, who promise won’t perform malicious MEV such as front-running

However, the RPC provider that the wallet is connected to can also be a public RPC provider, which sends the transaction to a public mempool. For example, the default RPC for Metamask is provided by Infura, which sends the transaction to the public mempool.

The searcher then runs a proprietary algorithm to find profitable MEV strategies, for example, cross-DEX arbitrage, and builds a transaction bundle that includes the target transaction with MEV opportunities and the transactions executed by the searchers that profit from the strategy.

The searcher then sends this bundle to builders , who might receive multiple bundles from different searchers.

Some bundles might be mutually exclusive, thus the builders also have to run an algorithm to pack the most profitable bundles by selecting the bundles that pay the most fees in a mutually exclusive bundle.

The most profitable bundles and other transactions in the mempool are packed as a block that is ready to be mined/proposed

The most profitable block is then sent to validators to be mined/proposed to the blockchain

In the current MEV landscape, the blocks are actually first sent to relays , which is a part of the MEV-boost design and acts as an aggregator of blocks

Each relay is connected to multiple block builders and receives packed blocks from each of the builders, the relay is responsible for picking the most profitable block for the validator and sending it to connected validators

Note that a validator can connect to multiple relays via MEV-boost

The relay is also responsible for a commit-reveal scheme to prevent validators from stealing the MEV opportunity

The relay will first only reveal the block header to the validator, which will then sign the header and sent the header back to relay

The relay will then send the full block content that includes the transaction to the validator

If the validator chooses to steal the MEV opportunity, which requires proposing a new block, the originally signed header will be published, and the validator will be slashed for double signing

3.2 Moat for each player

Wallet

The wallet is the first entity that receives transactions sent by the users. These transactions are valuable because they might contain MEV opportunities.

Wallet has the highest negotiating power in the supply chain, as it decides where the transaction will be sent, thus affecting who gets access to the valuable transaction order flow.